Protection of Personal Information Act 2013 and data protection for health research in South Africa

Ciara Staunton *, Rachel Adams**, Dominique Anderson ***, Talishiea Croxton ****, Dorcas Kamuya*****, Marianne Munene****** and Carmen Swanepoel*******

Key Points

- The Protection of Personal Information Act (POPIA) [No.4 of 2013] is the first comprehensive data protection regulation to be passed in South Africa and it gives effect to the right to informational privacy derived from the constitutional right to privacy.
- It is due to come into force in 2020, and seeks to regulate the processing of personal information in South Africa, regulate the flow of personal information across South Africa s borders, and ensure that any limitations on the right to privacy are justified and aimed at protecting other important rights and interests.
- Although it was not drafted with health research in mind, POPIA will have an impact on the sharing of health data for research, in particular biorepositories.
- It is now timely to consider the impact of POPIA on biorepositories, and the necessary changes to their access and sharing arrangements prior to POPIA coming into force.

Introduction

The right to privacy is constitutionally protected in South Africa (SA) by virtue of section 14 of the Constitution. As a corollary to that, section 32, which provides for the right of access to information by public and private bodies, also includes a right of access to personal information. The Protection of Personal Information Act [No.4 of 2013] (POPIA) is the first comprehensive data protection regulation to be passed in SA and it gives effect to this constitutional right to privacy. It is due to come into force in 2020 and seeks to regulate the processing of personal information in SA, regulate the flow of personal information across SA's borders, and ensure that any limitations on the right to privacy are justified and aimed at protecting other important rights and interests.

Although it was not drafted with health research in mind, POPIA will have an impact on the use and sharing of health data for research. Genomic research and biorepositories are dependent on accessing and sharing large quantities of biological samples and associated data. The growth of international collaborative projects such as HapMap, MalariaGEN, H3Africa and B3Africa has increased the sharing of genomic data across SA's borders, to other parts of Africa and the world. POPIA

* Ciara Staunton, School of Law, Middlesex University, UK; Institute for Biomedicine, Eurac Research, Italy, Email: c.staunton@mdx.ac.uk.
** Rachel Adams, Human Sciences Research Council, South Africa; Information Law and Policy Centre, Institute of Advanced Legal Studies, University of London, UK
*** Dominique Anderson, South African National Bioinformatics Institute, SA MRC Bioinformatics Unit, University of the Western Cape, South Africa
**** Talishiea Croxton, Institute of Human Virology, University of Maryland Baltimore, USA; Institute of Human Virology, Nigeria
***** Dorcas Kamuya, KEMRI-Wellcome Trust Research Programme, Kenya
****** Marianne Munene, KEMRI-Wellcome Trust Research Programme, Kenya
******* Carmen Swanepoel, Department Pathology, National Health Laboratory Services, Tygerberg Hospital; Faculty of Medicine and Health Sciences, Stellenbosch University, South Africa

The authors would like to thank Dr Simisola O. Akintola and the anonymous reviewer for comments on an earlier draft of this article.

will thus have considerable impact on genomic research and biorepositories, particularly on the purposes for which the genomic data may be processed, and the conditions under which it may be shared. It is now timely to consider the impact of POPIA on biorepositories, and the necessary changes to their access and sharing arrangements prior to POPIA coming into force.

The purpose of this article is to consider whether biorepositories in SA are meeting its data protection obligations using a small academic research biorepository in the Western Cape of SA as a case study. This article will first provide an overview of the development of biorepository research in SA. To ascertain whether this biorepository is meeting its current data protection obligations and is POPIA ready, it will analyse the regulation of data protection for biorepositories in SA to identify its duties and obligations in the use and reuse of health data for research and the policies of the biorepository to determine whether they are in line with national duties and obligations. As these data protection obligations impact on the sharing of health data outside of SA, the national and local data protection policies of a biorepository in Kenya and Nigeria will be analysed to determine if they meet the requirements under SA law so that biorepositories in SA can continue to share data with the coming into force of POPIA.

Overview and development of biorepository research in Africa

In 1990, the Council on Health Research for Development (COHRED) reported on the disparity between the burden of disease and health research investment. The report highlighted that less than 10 per cent of global health research funding was directed to conditions accounting for 90 per cent of the global disease burden.[1] In the past two decades, biorepository science has experienced above average growth, but it is vastly underrepresented in low and middle income countries (LMICs).[2] A 2016 bibliometric overview of over 20,000 biorepository records revealed that less than 2 per cent of authors publishing in the field were located in Africa.[3] Previously, storage facilities in Africa served as temporary sample repositories to developed countries, with scientific analysis conducted outside of the continent.[4] This uni-directional flow of samples resulted in exploitative research with little local oversight of the samples or research capacity development on the continent.

Early initiatives in biorepository science in Africa focused on disease-specific, or population-specific research, with much of the resources focused on the collection of samples for HIV/AIDS, Tuberculosis and Malaria research.[5] The Gambia established the first national databank for DNA in Africa in 2000[6] and a biorepository and pharmacogenetic database located in Harare, Zimbabwe was established in 2008.[7]

Alongside the need for high-quality biological samples for biomedical research endeavours, the increased size and complexity of biological data being generated in commercial and academic research environments has driven the need for capacity development (both human and infrastructure) in bioinformatics and computational biology. The application of bioinformatics to biomedical research provides deeper insights into fundamental biology in this 'omics' driven era.[8] In SA, bioinformatics was recognized as a critical skill early on, leading to the establishment of the South African National Bioinformatics Institute (SANBI) in 1996.[9] At the same time, the European Molecular Biology network (EMBNet) established the first bioinformatics node at SANBI and funding support from the World Health Organisation Special Programme for Research and Training in Tropical Diseases (WHO TDR) allowed for the establishment of the African Regional Training Centre for Bioinformatics and Applied Genomics in SA. In 2002, the Biotech Regional Innovation Centres were initiated and established by the South African Department of Science and Technology (SA-DST). Other initiatives aimed at bolstering world-class bioinformatics capacity in Africa included the establishment

1 Council on Health Research for Development, *Health Research: Essential Link to Equity in Development* (Oxford 1990) 157.

2 Jonas Astrin and Fay Betsou, 'Trends in Biobanking: A Bibliometric Overview' (2016) 14(1) Biopreservation and Biobanking 65.

3 Elizabeth Sarah Mayne and others, 'Genes for Life: Biobanking for Genetic Research in Africa' (2017) 15(2) Biopreservation and Biobanking 93.

4 Ibid.

5 Nagla Gasmelseeda and others, 'Sub-Saharan Centralized Biorepository for Genetic and Genomic Research' (2012) 423 Science of the Total Environment 423; Maimuna Mendy and others, 'Infrastructure and Facilities for Human Biobanking in Low- and Middle-Income Countries: A Situation Analysis' (2014) 81 Pathobiology 252; C Soo and others, 'Establishing an Academic Biobank in a Resource-challenged Environment' (2017) 107(6) South African Medical Journal 486. Jim Vaught, 'Biobanking and Biosecurity Initiatives in Africa' (2016) 14(5) Biopreservation and Biobanking 355.

6 Gasmelseeda, ibid.

7 Billie-Jo Hardy, and others, 'The Next Steps for Genomic Medicine: Challenges and Opportunities for the Developing World' (2008) 9 Nature Reviews Genetics S23.

8 Thomas Karikaria, Emmanuel Quansah and Wael Mohame, 'Developing Expertise in Bioinformatics for Biomedical Research in Africa' (2015) 6 Applied & translational genomics 31.

9 Nicola Mulder and others, 'The Development of Computational Biology in South Africa: Successes Achieved and Lessons Learnt' (2016) 12(2) PLOS Computational Biology e1004395. https://doi.org/10.1371/journal.pcbi.1004395

of global networks such as the African Society of Bioinformatics, the International Society for Computational Biology (ASBCB), and the National Institutes of Health (NIH) funded H3ABioNet. H3ABioNet is a pan-African bioinformatics network that is led from SA and supports over 30 continent-wide computational biology groups with human and infrastructure resource building.[10]

The increase in international health research projects, particularly those related to 'omics' is gaining momentum across the African continent. Huge efforts are underway to create global consortia of regional and national biorepositories in Africa with the aim to bolster biorepository science and increase awareness in genomics, biorepositories and bioinformatics, as well as ethical, legal and social issues associated with the research. The formation of various associations is contributing to building platforms in which African researchers are able to develop large interdisciplinary collaborations with others, strengthening existing north–south collaborative networks, while promoting valuable south-south networks.[11] Taken together, the prowess of African researchers is highlighted as they deliver world-class science and compete for more resources while mapping a pathway to health ownership on the continent.[12]

In SA, the complex and multidisciplinary science of biorepositories is driven by stakeholders on an academic, government, and commercial level. Responsibility for human biorepository activities falls under the mandate of the South African Department of Health (DoH) and the National Health Laboratory Service (NHLS).[13] While the exact number of functional biorepositories in SA is not immediately clear, it is estimated that over 12 biorepositories of different sizes are in operation, however, not all of these are specific to research.[14] It is important to note that many repositories which serve human research projects are 'personal' academic collections, with specimens collected for project specific capacity. The importance of any scientific collection to the South African Bioeconomy has been reinforced by the DST. The SA government has recognized the value of all collections, as national assets, irrespective of size or collection type and aims to ascertain the nature of these biorepositories with a view to ensuring adequate resources are in place for sustainability and maintenance. As with other regions on the African continent, the requirement for strategically located biorepositories on a regional and national level cannot be disputed, however, fundamental issues of governance, procedural harmonization, ethics and infrastructure remain important considerations.

Regulation of data sharing for health research in South Africa

POPIA will bring considerable changes to and the use and sharing of data for genomic and biorepository research in SA, but it does not exist in isolation. Rather, the regulation of data protection and sharing for genomic research and biorepositories in SA is currently regulated by the Constitution, the National Health Act [No. 61 of 2003], the Regulations Relating to the Import and Export of Human Tissue, Blood, Blood Products, Cultured Cells, Stem Cells, Embryos, Zygotes and Gametes 2012, the 2018 Material Transfer Agreement for the Transfer of Human Biological Materials (hereinafter referred to as the 2018 MTA Agreement), the 2015 DoH Ethics in Health Research**:** Principles, Processes and Structures Guidelines (hereinafter referred to as the 2015 DoH Ethics Guidelines) and any additional local health research ethics committee (HREC) requirements. This fragmented approach requires a complex navigation for researchers and industry, and at times lacks consistency. However together with POPIA, a full understanding of the regulations are necessary to ensure that biorepositories in SA are compliant with their data protection obligations.[15]

National Health Act [No. 61 of 2003] and supplementary regulations

The National Health Act [No. 61 of 2003] is the primary legislation governing the provision of health services in SA, and provides for the confidentiality of patient records as well as the regulatory framework for health research. The 2003 Act, together with its supplementary regulations provide some oversight on the access and use of health records in research, and the storage, access and use of genomic data for research.

The confidentiality of a health care user's information must be protected, unless they consent, disclosure

10 Ibid. Karikari and others (n 8).

11 Synthia Munung, Bongani Mayosi and Jantina de Vries, 'Equity in International Health Research Collaborations in Africa: Perceptions and Expectations of African Researchers' (2017) 12(10) PLOS ONE, e0186237. https://doi.org/10.1371/journal.pone.0186237

12 Hardy and others (n 7); Mendy and others (n 5).

13 Akin Abayomi and others, 'Challenges of Biobanking in South Africa to Facilitate Indigenous Research in an Environment Burdened with Human Immunodeficiency Virus, Tuberculosis, and Emerging Noncommunicable Diseases' (2013) 11(6) Biopreservation and biobanking 347–54. Pamela Andanda and Sandra Govender, 'Regulation of Biobanks in South Africa' (2015) 43(4) Journal of Law Medicine and Ethics 787.

14 Ames Dhai, 'Establishing National Biobanks in South Africa: The Urgent Need for an Ethicoregulatory Framework' (2013) 6(2) South African Journal of Bioethics and Law 38.

15 See also Andanda and Govender (n 12). Safia Mahomed and others, 'Managing Human Tissue Transfer Across National Boundaries – an Approach from an Institution in South Africa' (2016) 16(1) Developing World Bioethics 29; Dhai (n 14).

is mandated by a court, non-disclosure is a serious risk to public health (section 14), or disclosure is for a legitimate purpose and in the best interests of the health user (section 15). Each health establishment must have processes in place to prevent unauthorized access to a health user's health records (section 17). A health care provider can only obtain access to a health user's records for research if they obtain the consent of the health care user, and approval from the research ethics committee (REC) and head of the health establishment.

Health research generally is governed by Chapter 8 of the 2003 Act. Human tissue, blood or blood products cannot be removed without that person's consent (section 55) and informed consent is necessary prior to any research on human subjects (section 71). Research must be approved by a REC established under section 73. The Regulations Relating to Research with Human Participants 2014 provide more detail on the procedures to be followed for conducting human research, specifically section 5(g) requires that as part of the informed consent process, participants must be told about the extent to which their privacy and confidentiality will be maintained.

Regarding biorepositories themselves, SA lacks a coherent legislative framework for the establishment and governance of biorepositories, but a number of regulations do relate to research on human biological samples. The Regulations relating to the use of Human Biological Materials 2012 defines biological material as 'material from a human being including DNA, RNA, blastomeres, polar bodies, cultured cells, embryos, gametes, progenitor stem cells, small tissue biopsies and growth factors from the same'. Such material cannot be removed for genetic research without the consent of the individual (section 1(a)) and this research must be approved by a HREC (section 3(2)). If an institution conducts genetic research, it must keep a registry of that research (section 12). In addition, an institution that keeps or discloses genetic material records and 'other individually identifiable health information' must treat the information as confidential, ensure that users have access to their records, obtain informed consent before any other individual or body is provided with access, the information is treated as anonymous if used for research, the records are destroyed after the purpose for which they were created have been served and the written informed consent of the donor is obtained for 'long term storage of genetic material, stem cells or research findings'.

The Regulations Relating to Human Tissue Banks 2012 specifically relate to human tissue, but have implications for data protection and sharing. A donor management system must be put in place (section 6), and section 15 outlines the data protection and confidentiality responsibilities: a tissue bank must ensure that all data including genetic information must be kept confidential, put in place data security measures, protect the privacy and anonymity of donors, while guaranteeing the traceability of donors. Section 17 states that research must be conducted in accordance with Chapter 9 of the 2003 Act and approved by a REC, but it is envisaged that research will be conducted on tissue samples only and not data.

The Regulations Relating to Stem Cell Banks 2012 have similar requirements regarding privacy and confidentiality. Section 10 requires that all data including genetic information remains confidential, data security measures and procedures to resolve data discrepancies be put in place, no unauthorized disclosure of information occur, and the privacy and anonymity of donors are protected.

Material Transfer Agreement of Human Biological Materials 2018

In 2018, the Material Transfer Agreement of Human Biological Materials 2018 (GG 41781) (hereinafter 2018 MTA Agreement) was gazetted and set out a contractual template for the cross border flow of biological samples and data. Unlike the 2012 regulations, the MTA Agreement specifically applies to biological samples and data. It provides clarity as to the obligations of the different parties to the Agreement and specifically assigns responsibility to RECs, the providing institution, and the recipient institution. It also permits broad consent, provided the research is approved by a HREC.

It is the providing institution that remains the custodian of the materials (section 3.3) and it is their responsibility to obtain export permits (if necessary), obtain the informed consent from the donor, and obtain HREC approval (section 4). The recipient can only carry out research that has been approved by the HREC and cannot transfer any materials to any entity not specified in the MTA without the approval of the HREC (section 5). They also have the responsibility to ensure that the identity of the donors and the materials are kept secure and confidential.

It is the HREC at the providing institution that has an important oversight role. It is their duty to review and approve research that requires the transfer of materials, review and approve the MTA, review and approve all secondary research (ie use of materials for research other than uses determined in the approved research), and it is the last body to sign the MTA once it is satisfied that the provisions of the MTA have been met (section

6). This oversight function continues once the materials have been transferred and the approval of the HREC of the transferring institution must be obtained if the receiving institution wishes to use the materials for research that is outside of the MTA.[16]

Department of Health Ethics Guidelines 2015

In addition to this legislative framework, the National Health Research Ethics Council (NHREC) is mandated by section 72 of the 2003 Act to develop national ethics guidelines. These guidelines were revised and updated in 2015 (hereinafter referred to as the Department of Health Ethics Guidelines 2015)[17] and have particular provisions on the use of biological material and data for research purposes.

Section 3.3.6 requires informed consent prior to the use of data for research, and this is interpreted as including specific, broad and tiered consent. It is for the HREC to determine the appropriateness of the consent model in the protocol and the circumstances in which re-consent will be necessary. Secondary use of data (defined as 'use in research of materials or data originally collected for other purposes') is permitted under certain circumstances and it is for the HREC to determine if a new consent is necessary.

Genetic research is given specific attention in the guidelines and section 3.3.8 requires HRECs to consider privacy and confidentiality, amongst other factors. The guidelines caution that additional protections for participants may be necessary in instances where identifiable data and samples are collected. In addition, section 3.1.8 discusses the privacy and confidentiality interests that must be considered when an HREC is making a review: a protocol must describe how data records are to be secured, duration of retention and who is responsible for storage and disposal. The 2015 Guidelines note the passing of POPIA and that HRECs and researchers should 'pay careful attention to measures that will protect privacy and confidentiality interests'.

The foregoing legislation, regulations and guidelines are specific to health research, but there are two additional general legal frameworks that are more general but pertinent to the regulation of health data for research: The Promotion of Access to Information Act 2000 and the Protection of Personal Information Act 2013.

Promotion of Access to Information [Act 2 of 2000]

In 2000, the Promotion of Access to Information Act (PAIA) was signed into law, giving effect to section 32(a) and (b) of the Constitution which provided for the right of access to information and the promulgation of legislation to govern the rules of disclosure and exemption. When the PAIA came into effect it was the first access to information law on the African continent, and one of the first access to information laws globally to provide for a right of access to records held by private bodies. Following section 32 of the Constitution, access to privately held records is permitted on the basis that the information is required for the exercise or protection of another right. Notably, as was later decided in the case of *Van Niekerk v Pretoria City Council*, 'rights' in this context referred not just to the rights set out in the Bill of Rights, Chapter 2 of the Constitution, but all common law rights.[18]

PAIA can be understood as the precursor for POPIA insofar as the PAIA sets out a number of provisions in terms of compliance with the Act by public and private bodies, and access requests, which are then included in POPIA. Thus, while POPIA has been seen to *revoke* various aspects of the PAIA, it may be more accurate to say that POPIA *develops* a number of the provisions set out in the PAIA. These developments and continuities in terms of compliance and information requests, will be discussed in detail below, following an overview of the PAIA.

The PAIA sets out the procedures for accessing information held by public and private bodies, and a series of categories of information which are exempted from disclosure, in line with its objectives of contributing to 'an open and democratic society' set forth in the Preamble. The exemptions from disclosure are categorized under the Act in terms of mandatory exemptions, whereby the Information Officer must refuse the access to information request, and discretional exemptions, whereby the Information Officer must weigh up the potential harms and prove that disclosure would cause greater harm to the public or private body if deciding in favour of non-disclosure. The grounds of mandatory exemption from disclosure under PAIA include commercial information of a third party (sections 36 and 64), confidential information (sections 37 and 65), research information (sections 43 and 69), as well as

16 For more on the transfer of samples outside of SA, see Ciara Staunton and Keymanythri Moodley, 'Data Mining and Biological Sample Exportation from South Africa – a New Wave of Bio-Exploitation under the Guise of Clinical Care?' (2016) 106(2) South Africa Medical Journal 136–38.

17 South African Department of Health, *Ethics in Health Research: Principles, Processes and Structures* (2nd edn, 2015).

18 *Van Nikerk v Pretoria City Council* 1997 (3) SA 839 (T).

information which 'would involve the unreasonable disclosure of personal information about a third party' (sections 34 and 63). To date, what constitutes an '*unreasonable*' disclosure of personal information has not been specified by the courts. However, it is likely that in such circumstances the courts would defer to the provisions set out in POPIA, as the overriding legislation governing the disclosure and processing of personal information.

While the PAIA provides that the designated information officer must refuse requests for information where the records in question contain personal information, there are a number of circumstances whereby this exemption can be applied discretionally. These circumstances include personal information of an individual who has given consent for this information to be released, personal information which has already been made public and personal information of an individual who is or was an official of a public or private body and where the information relates to their position as an official.[19]

In addition to the above provisions, sections 46 and 70 of the Act set out a public interest override clause which means that all the conditions of exemption from disclosure, including on the grounds of personal information, can be overridden where the public interest of the information 'clearly outweighs the harm contemplated in the provision [of exemption to disclosure] in question'. In these circumstances the public interest of the information is determined by whether its disclosure would show a 'substantial contravention of or failure to comply with the law' or 'an imminent and serious public safety or environmental risk' (sections 46 and 70). The PAIA's public interest override clause was a critical reason why the Act was spoken of as 'a fairly radical law',[20] and influenced the development of the public interest override clause in the African Union's Model Law on Access to Information in Africa.[21] This provision has also been used in the past to gain access to information contained personal information in the case of *Centre for Social Accountability v Secretary of Parliament.*[22]

With regard to the above provisions relating to where personal information *may* be disclosed, the information officer dealing with the request must show evidence to prove that the information is not of public interest *and* would cause a greater harm if disclosed, if deciding in favour of non-disclosure. In addition, if the information officer decides to grant access to information that includes personal information, including research information in terms of section 43(1), all third parties whose personal information is contained in the disclosed records must be duly notified. The provisions above granting discretional disclosure of personal information would need to be read alongside the provisions for data processing set out under POPIA, discussed below, as POPIA is constitutionally the overriding law governing personal information.

There are a number of ways in which POPIA revises the PAIA. POPIA seeks to regulate the processing of personal information and, in doing so, serves both as an enabling legislation for the right to privacy and augments the provisions relating to the disclosure of personal information listed under the PAIA. Those developments most pertinent to the question being analysed here regarding the sharing of health-related data for research purposes, will be discussed.

Firstly, the PAIA's definition of what constitutes personal information changes to fall in line with the POPIA. This includes two key changes: the addition of biometric information as a category of personal information, and the clarification of personal information relating only to living persons. Largely, however, POPIA takes the wording of its definition of personal information from the PAIA.

Secondly, and perhaps most fundamentally, is that POPIA rescinds the powers of the South African Human Rights Commission as the oversight body for monitoring compliance with the PAIA and managing related complaints, and transfers these powers to the Information Regulator, established under section 39 of POPIA and discussed in further detail below. While this constitutes a major change in the oversight regime for access to information requests, the compliance procedures the PAIA sets out for public and private bodies remains the same in POPIA. These include: development of manuals which set out what categories of information (and personal information) a public or private body holds and how to make a request for information (and under POPIA how to make a request for changing or deleting personal information) (sections 14 and 51 of PAIA, and set out in section 17 of POPIA and section 4 relating to the duties of information officers in 2018

19 S 34 of PAIA. See Rachel Ward and others, South African Human Rights Commission: Guide on How to Use the Promotion of Access to Information Act 2 of 2000 (2014) <https://www.gov.za/sites/default/files/gcis_documents/SAHRC-PAIA-guide2014.pdf> accessed 17 June 2019.

20 D McKinley, 'The State of Access to Information in South Africa' Centre for the Study of Violence and Reconciliation. Cape Town, South Africa (2003).

21 S 25 African Commission on Human and Peoples' Rights (2012). Model Law on Access to Information for Africa.

22 *Centre for Social Accountability v Secretary of Parliament* 2011 (5) SA 279 (ECG).

POPIA Regulations); and the designation of information and deputy information officers to handle information requests (section 17 of PAIA, and section 56 of POPIA).

These compliance functions are important here for assessing how POPIA ready South African biorepositories are, as the first step to assessing this would be to ascertain how the PAIA compliant such bodies are. This could be readily assessed through ascertaining whether such biorepositories had publicly available the PAIA manuals which detailed contact information for their Information and deputy Information Officers, details of how an information request could be made, and details of what categories of information the biorepository holds.

The third key development relates to the manner through which requesters can request access to their personal data. Prior to POPIA, 'personal requests' as they were designated under the PAIA could access records containing their personal information through the procedures for access to information held by public or private bodies set out in the PAIA. While accessing information containing personal information will remain the same with the promulgation of POPIA, requesters seeking access to their own personal information can now do so under the procedures set out under the newly gazetted POPIA regulations of 2018.[23]

The Protection of Personal Information Act [No.4 of 2013]

The purpose of POPIA is to give effect to the constitutional right to privacy and regulate the processing of personal information 'in harmony with international standards' (section 2). It applies to any responsible person who is domiciled in SA or, if they are not domiciled in SA, 'makes use of automated or non-automated means in SA' (section 3(b)). Personal information is defined as information relating to 'an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person'. This includes a person's medical history, their race, gender, physical or mental health and biometric information (section 1). Thus, information collected from the data subject as well as any data derived from a biological sample comes under this definition, but it does not apply to de-identified personal data that cannot be identified again (section 6(1)(b)). An independent Information Regulator is established under section 39 and it is tasked with educating on the parameters of the Act, monitoring and enforcing compliance, consulting with interested parties, handling complaints, develop codes, and facilitating cross-border corporation (section 40).

POPIA sets out eight conditions for the lawful processing of personal information: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation. Under section 26 there is a general prohibition on the processing of 'special personal information' and this includes biometric information. This prohibition is subject to the following exemptions: if the data subject has consented to such processing (section 27(2)(a)); if the processing is for research purposes that either serve a public interest, or where it would be impossible or involve a disproportionate effort to ask for consent (section 27(2)(d)); or if the Information Regulator has provided authorization that processing is in the public interest and appropriate safeguards have been put in place (section 27(3)). Special authorization is also provided under section 32 for medical professionals and healthcare institutions to process special personal information in certain circumstances and states that 'personal information concerning inherited characteristics' can be processed for research purposes.

Genomic research and the establishment of biorepositories can thus continue in SA, but POPIA contains a number of provisions that will potentially have an impact on the operation of biorepositories and genomic research in SA.[24] In the collection of data and samples, biorepositories often collect more data than may be necessary, but the purpose specification requirement under section 13 requires personal data to be collected for a specific purpose. However, biorepositories often use data and samples for purposes not anticipated at the point of collection. Under POPIA, the further processing of the data is permitted provided it is compatible with the original purpose for which it was collected (section 15(1)). POPIA does not provide a definite list as to what constitutes 'compatibility', but it does identify times when data can be processed for purposes that were not in the original specific consent. Of particular importance for genomic research and biorepositories, further processing of data is not incompatible with the purpose of collection if processing is necessary to 'prevent or mitigate a serious and imminent threat to'

23 Government Gazette No R. 1838 (14 December 2018) Regulations Relating to the Protection of Personal Information under the Protection of Personal Information Act, 4 of 2013. <http://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf> accessed 31 May 2019.

24 See also Ciara Staunton and Elizabeth de Stadler, 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) 109(4) South African Medical Journal 232.

public health (section 15(3)(d)(i)) or 'the life or health of the data subject or another individual' (section 15(3)(d)(ii), if the information is to be used for research purposes and 'will not be published in an identifiable form' (section 15(3)(e)), or if the Information Regulator grants an exemption under section 37 (section 15(3)(f)). Such an exemption will be granted to a responsible party if the Information Regulator is satisfied that it is necessary for the public interest, which would include research.

Reading these sections together, the secondary use of personal information for a purpose that is not specified in the original consent is only permitted if the processing is for research that is intended to improve health, provided that the information will not be published in an identifiable form. In publishing the results of the research, research subjects must be de-identified, which under the POPIA means that all information that identifies a data subject, data that can be used by a reasonably foreseeable method to identify the data subject, or can be linked by a reasonably foreseeable method to other information that identifies the data subject, must be removed (section 1). This applies both to publication in journals and the availability of genetic information in a publicly accessible database.

On the face of it, the specificity requirement would appear to permit specific consent only. However, it has been argued that a purposive interpretation of POPIA demonstrate that POPIA permits the use of broad consent for research purposes, and such an interpretation is in line with the current legal–ethical framework for the governance of genomic research and biorepositories in SA.[25] Such an interpretation looks at the purposive of the legislation and in particular section 2 which states that the purpose of the legislation is to give effect to the constitutional right to privacy by safeguarding personal information, subject to limitations that seek to protect 'important interests, including the free flow of information within the Republic and across national borders'. Although POPIA does not contain an explicit research exemption, the importance of research is recognized and the responsible party is exempt from many of the strict provisions of POPIA, including restriction on retention of records (section 14), duty to notify (section 18), and prohibition on processing of special personal information (section 26) if the processing is for research purposes. Thus, it can be argued that research is an important public interest and the requirement of specific consent would undermine that research. Furthermore, requiring the specific consent would also undermine the free flow of information within SA and across its borders.[26]

Condition 2 (ie processing limitation condition) does put further limitations on the processing of personal information. Section 10 requires that personal information can only be processed if it is adequate, relevant and not excessive. Thus, when collecting personal information, biorepositories must only collect information that is relevant to research and not excessive. Under section 12(1) the personal information must be collected from the data subject. Considering the extent to which data is shared amongst biorepositories, this would be of concern, but there are some exceptions in section 12(2) and they include when the data subject has consented to the collection of the information from another source, the collection of the information from another source would not prejudice the legitimate interest of the data subject, or where this would not be 'reasonable practicable in the circumstances of the particular case'. Thus, a biorepository can process data if a data subject consented to its use by other parties, or it would not be reasonably practicable to obtain the consent.

POPIA does require that records of personal information must not be retained for longer than necessary for achieving the purposes of the processing (section 14(1)). Such a requirement would limit the value of the personal information for research, but POPIA does provide some exceptions to this rule. Notably for biorepositories, personal information can be kept for longer if the data subject consents, or if the retention of personal information is for research purposes and there are 'appropriate safeguards' in place to stop the personal information from being used for any other purpose (section 14(2)). Such safeguards including technical and security safeguards discussed under section 19.

Rights of the data subject

POPIA provides for a number of rights and responsibilities. Looking first to the rights, we see that POPIA provides for a number of rights for the data subject, namely the right to notification, right to access, right to object, right to correction and deletion, and a right to redress. These rights seek to provide the data subject with control over their personal information, but they may be limited if the processing is for research purposes.

25 Ciara Staunton and others, 'Safeguarding the Future of Genomic Research in South Africa: Broad Consent and the Protection of Personal Information Act 2013' (2019) 109(7) South African Medical Journal 468.

26 ibid.

Under section 18(1) the data subject has a right to notification. It provides that, amongst other things, a responsible party must take 'reasonably practicable steps' to make the data subject aware that their information is being collected and where it was collected (where the information is not collected by the data subject), the purpose for collection, the fact that the responsible party intends to transfer the data to a third country, the level of protection afforded to information in that country, and the existence of other rights. However, compliance with this section is not necessary if the information is to be used for research purposes.

A data subject has the right to request from the responsible party whether they hold personal information about the data subject, including the identity of all third parties who have access to the information and be provided with a 'record or a description' of the personal information 'in a form that is generally understandable' (section 23(1)). Section 23 further provides that Information Officers must handle such requests in line with the categories for exemption from disclosure set out in the PAIA. These exemptions from disclosure are noted in the section above. The Information Officer deciding on whether to provide access to such information must also ensure compliance with the public interest override clause, detailed above. Section 11(3) provides the data subject with the right to object to the processing of their personal information 'on reasonable grounds relating to his, her or its particular situation' unless the processing is required by legislation. A data subject has the right under section 24 to request a responsible party to correct or delete personal information that is inaccurate, irrelevant, out of date, excessive, misleading, obtained unlawfully, or personal information that they are no longer authorized to retain. The Responsible Party then has to correct the information, or alternatively, destroy or delete it. This is not the same as the right to be forgotten under the GDPR and only applies to the personal data that a biorepository is currently processing.

When POPIA was originally promulgated, it detailed that data subject requests, such as those described under sections 23 and 24, must be made in terms of the procedures for access set out under the PAIA (as noted above). However, in December 2018, the Department of Justice and Constitutional Development issued a Regulation under the POPIA that provided a series of Forms to be used for making requests under Section 23 and 24, as well as making complaints in relation to the Act.[27]

Additionally, under the PAIA, requesters requesting access to records containing their personal information (known under the PAIA as 'personal requesters'), were exempt from paying a fee for access. Section 23(1)(b)(ii) of POPIA, however, makes provision for responsible parties to prescribe fees for requests made in terms of section 23, which at first reading appears to contradict the sentiment reflected in the PAIA. In the newly promulgated POPIA Regulations gazetted in December 2018, no mention is made of fees.[28] This would be an important point for the Information Regulator to clarify, particularly given the socio-economic circumstances of many living in SA, who may be excluded from exercising their right to privacy should responsible parties be granted the liberty to set access fees.

A data subject has the right to make a complaint to the Information Regulator under section 74 concerning an alleged interference with the protection of their personal data, and this includes a breach of a data subjects' rights. Chapter 7 sets out the procedures that the Information Regulator will follow when dealing with such a complaint. While this is to be welcomed, exercising their rights and instituting a complaint is contingent on a data subject being aware that their personal information is being processed. The right to notification is the only right that has a research exemption. Thus, if the lawful basis of processing is on any one of the grounds other than consent, a data subject may not be aware of the processing of their personal information for research purposes. This will include the secondary use of research under broad consent. A biorepository may apply the research exemption and they will be under no obligation to inform the data subjects of the use of their personal information in research, thereby making it virtually impossible in practice to exercise their other rights.

Responsibility for compliance with POPIA

Overall responsibility for the lawful processing of personal information and compliance for a biorepository falls to the Responsible Party (section 8) and the Information Officer (IO). It is the Responsible Party who determines the 'purpose of and means for processing personal information' (section 1), while the IO must encourage compliance (section 55).

27 Republic of South Africa, Department of Justice and Constitutional Development (14 December 2018) 'Information Regulator: Protection of Personal Information Act, 2013: Regulations Relating to the Protection of Personal Information' Government Gazette No R. 1383: <http://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf> accessed 17 June 2019.

28 Ibid.

Under section 19(1) the Responsible Party has the duty to secure the 'integrity and confidentiality' of personal information and to take 'appropriate, reasonable technical and organisational measures' to prevent loss of or damage of personal information or unlawful access or processing. As part of this, the Responsible Party must undertake a risk assessment and identify all reasonably foreseeable internal and external risks, establish and maintain appropriate safeguards against the risks, ensure that the safeguards are implemented, and ensure that they are updated in response to new risks (section 19(2)). Section 19(3) requires the Responsible Party to have due regard to the generally accepted security practices and procedures that may apply to a specific industry or professional rules and regulations. If the Responsible Party has reasonable grounds to believe that personal information has been acquired by an unauthorised person, they must inform the Information Regulator and the data subject (section 22(1)). They also have obligations regarding data quality and must take 'reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary' (section 16).

Under section 55 an IO is to be appointed and registered by the Responsibility Party with the Information Regulator before it can take up its role. All public and private bodies in SA should already have an appointed IO as required under the PAIA. It is envisaged that the PAIA appointed IO's will assume the new responsibilities assigned to them under the POPIA. The IO is expected to encourage compliance, deal with any data requests and be involved in any investigation by the Information Regulator. The responsibilities of the IO are further elaborated in the 2018 Regulations and they include ensuring that a compliance framework is developed, implemented, monitored and maintained, a personal impact statement is done, a manual is developed, monitored, maintained and made available as prescribed in PAIA, develop procedures to adequately process request for information and conduct awareness sessions regarding data protection internally.[29]

Section 55 brings clear lines of accountability and by acting as a conduit, the IO can ensure that research institutions are accountable to the data subject and the Information Regulator. Outside of this, the POPIA offers very little guidance on the IO, the qualifications or experience required, whether the IO can be involved in the processing of personal information or if it can be contracted out. The Information Regulator must develop a job description detailing the duties and responsibilities of the IO as well as a person specification. Concerns have been expressed that failure to do so risks the responsibility of the IO falling to someone currently within the institution that may not have the necessary skills, experience or time.[30]

Cross border transfer of data

POPIA starts from the premise that transfer of personal information outside of SA is not permitted, but does provide for exemptions. Notably for research, under section 72 the exceptions include if the party in receipt of the information is subject to a law, binding agreement, or binding corporate rules that provides a level of protection that provides for substantially similar conditions to the processing of personal information and includes provisions that are substantially similar to the further transfer of personal information from the recipient to a third country (section 72(1)(a)), or the data subject consents to the transfer (section 72(1)(a)). Section 57(1)(d) also mandates that the Responsible Party must obtain the prior authorization of the Information Regulator if it intends to transfer special information (of which genetic information falls under) to a third country 'that does not provide an adequate level of protection for the processing of personal information as referred to in section 72'.

In the context of genomic research and biorepositories in SA there is anecdotal evidence to suggest that many consent forms have not specifically included the cross-border transfer of data. Thus, biorepositories will need to ensure that there are laws or agreements in place that provides for the same level of protection as under POPIA. As many African jurisdictions have not implemented data protection legislation, it will fall to a binding agreement, most likely in the form of an MTA and/or a data transfer agreement (DTA), to ensure compliance with section 72.

The regulation of health data in South Africa: issues for a biorepository to consider

The coming into force of POPIA will bring a number of changes to the use, re-use and oversight of data for health research in SA, but biorepositories in SA must be mindful of their other duties under the currently regulatory framework. Table 1 provides a useful overview of all the regulatory requirements once the POPIA comes into force.

29 Ibid.

30 Staunton and others (n 25).

Table 1: Regulatory requirements for biorepositories in SA

Consent	• Informed consent is necessary for all research; • Broad consent is permissible for genomic research and biorepositories; • Re-consent for secondary use necessary if required by the HREC; • Consent for processing of genetic information necessary unless it is to be used for research and would require a disproportionate effort, or the Information Regulator provides authorisation, or it is in the public interest; • Data subjects must be informed about how their privacy and confidentiality will be protected.
HREC	• Must approve all research; • Must ensure that protocols describe how data records are to be secured; • Must consider privacy and confidentiality interests in protocols; • Must determine if broad consent is permitted and if re-consent is necessary; • Approval necessary for the secondary use of data; • Final entity to approve and sign the MTA; • Responsible for oversight of the MTA; • Must approve any subsequent use of data that falls outside of the remit of the MTA, including any further transfer of data; • Approval necessary for research that requires the transfer of data outside of SA.
Responsible party	• Ensure data is only processed based on one of the lawful grounds for processing; • Processes in place to facilitate the right to notification, the right to access, the right to correction, the right to object, and the right to notification; • Establish appropriate safeguards to address any risks; • Update these safeguards where necessary; • Have processes in place so that they inform data subjects and the Information Regulator in the event of a data breach; • Must appoint and seek approval from the Information Regulator and Information Officer.
Information Officer	• Undertake a data protection risk assessment; • Ensure a compliance framework is developed; • Ensure a manual is developed as prescribed under PAIA; • Develop procedures to process requests for information.

Regulation of data sharing and protection at a biorepository in the Western Cape

The NHLS Stellenbosch University Biorepository (NSB) is a small academic biorepository situated within the Division of Haematology and is affiliated with both the NHLS and Stellenbosch University (SU) at Tygerberg Hospital, Cape Town, South Africa. Its purpose is to manage, process and preserve high-quality biological samples, maintain effective sample transport logistics, implement cost effective and innovative technology for preservation and transportation and focus on the science of cryopreservation. It has established risk management & emergency plans and has experience in sample logistics management across Africa, Europe, the UK and the USA. The NSB is capable of processing, performing sample quality control and storage of various biospecimen types from blood and its derivatives, DNA/RNA, saliva, tissue, urine and cell lines. Most aspects of operations are computerized and integrated into a Laboratory Information Management System (LIMS) system to allow for monitoring and evaluation of biorepository operations, biological samples and data tracking and storage. In addition to the national legislation, regulations and ethical guidelines, the NSB also comply with local guidelines as well as National Cancer Institute (NCI) and International Society for Biological and Environmental Repositories (ISBER) best practices and relevant H3Africa and B3Africa policies.

The establishment and registration of a biorepository at SU requires specialised biorepository and/or database registry application forms with the submission of a number of documents to the SU HREC. These include the Standard Operating Procedures (SOP) Masterlist that covers all essential biorepository operating SOP's and workflows, records management plans, workflows related to biorepository operations, transport and

shipping guidelines, training and certification documentation of staff related to Good Clinical Practice (GCP), Good Clinical Laboratory Practice (GCLP), International Air Transport Association (IATA) certification as well as proficiency testing, overview of operational and management governance workflows, infrastructure and capacity plans, risk management and disaster recovery response plans, sustainability plans, the informed consent form, a flow chart depicting the process of data accrual and release, H3A developed and implemented template application form for access to data as well as the Data and Biospecimen and Access Committee policy, and a draft MTA.

The SU HREC has two consent form templates: a general patient information leaflet and consent form and a consent form for genetic studies. Although the template suggests risks to be discussed with the participant, there is no mention of risks to privacy or confidentiality under the general risks section. A separate section is devoted to confidentiality and its importance, particularly if the biological sample is to be exported. The template states that participants should be told if the sample is to anonymised, how the data is to be de-identified, who has access and how this is to be protected in terms of infrastructure access. Generally, the emphasis in the consent form is on the biological sample, with little attention given to genetic data and data generally. The general consent form requires additional information including who may have access to the participant's medical records and that information will be treated as confidential and protected.

The NSB consent form stresses the voluntariness of participation and that the participant can withdraw their consent at any time. It informs the participant that sample and medical information will only be provided to researchers after the independent access committee has approved researchers' requests to use the stored samples if samples are donated and for sharing purposes. Most samples stored are specific for research projects and/or consortia with their own specific access committees. In most cases it is just for sharing within the particular consortium and for use for a specific researcher, but this is not specified in the consent form. The NSB consent form states that minimal clinical information may be provided to the NSB and added to their database, but no name or information that could personally identify the participant will be included. To protect the confidentiality of participants, they are told that their sample will be coded and all personal identifiers will be removed, but that there is a risk that genetic information could be used to trace the participant. The NSB does not keep any identifying information that links participants to particular samples.

The SU HREC MTA Template Term Sheet requires a justification for receiving or providing data, the name and contact details of the PI and other organizations involved in the MTA, the entity that is the custodian of the data, potential uses of the data that have already been identified, the uses of the data by the recipient, timeframe for use of data, and a description of what will happen to the data after the completion of the study. The MTA must be drafted and approved by the SU Research Contracts Office, and the MTA must be returned to the HREC for approval only if 'after HREC approval of this MTA Term Sheet the MTA differs *substantively*, the Researcher shall submit the MTA to HREC to enable review prior to signature of the MTA'.

The SU Privacy Regulation aims to articulate SU's institutional stance on privacy, support efforts to give effect to the constitutional right to privacy within Stellenbosch University, and support the management of risks and opportunities surrounding personal information processing. It is been approved by SU senate February 2019 and implemented in March 2019 with the purpose to bring SU in line with POPIA and establish an institutional framework 'that positions respect for data subjects, transparency, accountability, and auditability at its core'.

Data protection at the NSB: some observations

The NSB has a number of policies and forms that impact data protection, but overall improvements must be made to ensure that it can meet its legal requirements. First changes must be made to the consent form. Although the NSB consent form does provide more information to the participant, it (along with the SU template consent form) is too focused on the biological sample, with little consideration given to the issues that may arise in deriving, using and sharing genetic data from the sample. The consent forms must be amended to provide more information on the derivation, use and sharing of genetic data. Furthermore, the NSB must make clear how it will process requests for access to genetic data.

Secondly, the SU MTA is also not in line with the national MTA template. Under that template, it is the REC that is responsible for oversight of the MTA and must be the last entity to approve the MTA. The SU MTA places greater emphasis on the role of the Research Contracts Office and the HREC will only receive it if it differs substantively from the template it received in the protocol. To align itself with the national

MTA template, after approval from the Research Contracts Office, the NSB must seek final approval from the HREC. The NSB must also ensure that there will be no subsequent use of the data for purposes not specified in the MTA without approval of the HREC. The SU template also neglects to require that, if exporting data, the receiving institution has similar protections in place for data subjects as that provided under the POPIA. Thus, the NSB should develop a template MTA that is used when exporting data to ensure that the receiving institution provides the same level of protection as that under the POPIA.

Thirdly, in relation to the NSB's obligations under the PAIA, SU has a PAIA Manual available for public access on its website, which includes details of its IO and Deputy IO. However, this manual is extremely broad and does not provide information relating to whether SU subsidiary bodies—such as the NSB—would be considered a public or a private body under PAIA and how information held by such bodies could be accessed and what kinds of information such bodies hold.

Finally, the SU Privacy Regulation when implemented by the NSB will go some way to ensuring that SU is compliant with POPIA. The policy must ensure that its focus is not just on institutional data, but it should also consider the implications of POPIA on data for research. Considering health data for research is at times treated different from institutional data under POPIA, the NSB would be best advised to push for a similar regulation for research. In the interim, the NSB should conduct a privacy impact assessment as outlined in the regulation and implement the necessary changes recommended in this assessment to ensure that the NSB meets its data protection obligations.

The regulation and protection of data sharing for health research in Kenya

The NSB is also involved in the sharing of biological samples and data with the Kenyan Medical Research Institute (KEMRI). The right to privacy in Kenya is protected by Article 31 of the Constitution of Kenya and Article 35 which provides for the right to access information. The Access to Information Act No. 31 of 2016 gives effect to the right to access information, but there is currently no legislation to give effect to the right to privacy. The Access to Information Act, however, includes a number of provisions relating to the protection of personal information, including: section 13 which provides for the correction or incorrectly held personal information; section 21(1) which provides for the responsibilities of the Access to Information Commission which includes 'the protection of personal data'; and section 25(2)(h) which provides that the Minister may prescribe regulations for procedures to the erasure of personal information held by public or private bodies. That being said, the definition of personal information relating to biometric information includes only 'blood type' and 'fingerprints' (section 1). Data protection is however currently receiving considerable attention and discussion in Kenya due in part to the establishment of a National Integrated Identity Management System (NIIMS) that is seeking to gather the biometric data of its citizens and link it to government services. Furthermore, although focusing on the privacy implications of biometric voter registration, a 2018 Report highlighted the need for data protection legislation to operationalise this right to privacy.[31] Data security concerns and the lack of a national data protection policy were identified as threats in the Kenya National E-Health Strategy.[32] Thus the Data Protection Bill that is currently making its way through parliament is to be welcomed.[33] This Bill will impact the sharing of data for biorepositories and will be in addition to the regulations that exist pertaining to health research.

Regulation of health research in Kenya

The Science, Technology and Innovation Act 2013 seeks to regulate science, technology and innovation in Kenya. The Kenya Medical Research Institute (KEMRI) was established by the Science and Technology (Amendment) Act of 1979 and it is the national body responsible for carrying out research in Kenya.

Under the recently enacted Health Act 2017, research is clearly given priority in Kenya and section 4(b) provides that it is a fundamental duty of the State to prioritize and provide adequate funding for health research. The Act places a number of wide-ranging duties on the Ministry for Health, including developing and expanding a national health information management system (section 15(r)) and facilitate research that advances the interest of public health (section 15(s)). The importance of protecting the confidentiality and privacy of patients are raised. Section 5(2) states that the right to privacy must be respected in accordance with the Constitution and the Act (section 5(2)), and in the research context,

31 <https://blog.cipit.org/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf> accessed 31 May 2019.

32 Kenya National e-Health Strategy 2011–2017, p 5.

33 <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2018/DataProtectionBill_2018.pdf> accessed 31 May 2019.

section 11 prohibits the sharing of patient information, including information relating to their 'health status, treatment or stay in a health facility' without the patient's consent.

Section 93 provides for the establishment of a National Health Research Ethics Committee whose purpose is, amongst others, 'make recommendations on the development on the national research for health policy'. Section 99 states that research involving 'human subjects' should follow the regulatory requirements as set out by the Commission for Science, Technology and Innovation, and that the National Health Research Committee (NHRC) shall set ethical standards for health research approvals. However, the NHRC has not yet been constituted and currently the National Council for Science, Technology and Innovation (NACOSTI) has the mandate to ensure that the standards for responsible conduct of research in the country are upheld through the National Bioethics Committee (NBC). The NBC is responsible for setting ethical standards and accreditation of RECs in Kenya. Given the substantial number of protocols submitted each month in the entire country, the NACOSTI has devolved ethic review to accredited RECs that meet some minimum standards. The accredited RECs then serve on behalf of the NACOSTI and the national REC. The accreditation lasts for 2–3 years and the accredited REC is assessed on performance and whether they meet the national standards, otherwise the accreditation can be revoked. All research in Kenya must be approved by an accredited REC, even if it is just minimal risk. The NACOSTI thus has oversight over RECs in Kenya. In addition, any KEMRI unit must follow the KEMRI Scientific and Ethics Review Unit Standard Operating Procedures (SERU SOPs).[34] The ethics review must consider the adequacy of proposals to protect the confidentiality of data.

The 2004 National Council for Science and Technology 'Guidelines for Ethical Conduct of Biomedical Research Involving Human Subjects in Kenya'[35] are legally enforceable guidelines as mandated by the Science, Technology and Innovation Act 2013 and they provide further guidance on the ethical oversight of medical research in Kenya. It places emphasis on certain key values including informed consent and independent review. The Guidelines state that as part of informed consent participants must be individuals must be 'accurately informed of the purpose, methods, risks, benefits and alternatives to the research'. Informed consent can be waived by an ethics committee if it is minimal risk (defined as 'risk not greater than that attached to routine medical or psychological examination') and/or it is not practical to obtain informed consent (example given is research that extracts data from patient records). The Guidelines further note that for some epidemiological studies that use left-over 'anonymous' biological samples or patient records, it is for the ethics committee to decide whether the investigator has put in sufficient safeguards to protect the privacy of the participants and the confidentiality of the data when deciding whether to waive informed consent.

The KEMRI Scientific and Ethics Review Unit (SERU), one of the NACOSTI accredited RECs, have SOPs on informed consent, secondary use of samples, genetic research and the import and export of samples, amongst others. The informed consent SOP and secondary use of samples SOP[36] provides guidance on the use of archived samples and under section 25.3 samples can be collected using broad consent 'provided that the samples will be anonymized or coded and the research is being conducted in line with the objectives of the initial study for which the samples were collected or a justified public health concern'.

The SOP for genetic studies require investigators to explain how rights will be protected and mandate that privacy and confidentiality protection measures be put in place. The SERU must be informed of all of those who have access to the identifiable data of study participants. Section 11.2.m provides detail on the use of genetic material, but this section focuses on the biological sample only and not the data. Section 24 provides guidance on the storage and shipment of biological samples, but again these pertain to the samples only and not the data.

KEMRI has guidelines on transfer or secondary use of biological samples. Each KEMRI centre has formalized MTAs and MTA templates that have been used in any processes that require shipment of samples out of the country. In line with ongoing revisions of guidelines and SOPs by NACOSTI, KEMRI SERU is also revising its policies and harmonizing the MTA templates across its 12 centres.

34 KEMRI Scientific and Ethics Review Unit Standard Operating Procedures (SERU SOPs) Version 1.0 Dated 27-September-2016 (<https://www.kemri.org/images/joomlart/documents/Final%20SERU%20SOPs_27%20Sep%202016%20(3).pdf> accessed 31 May 2019).

35 National Council for Science and Technology, 'Guidelines for Ethical Conduct of Biomedical Research Involving Human Subjects in Kenya' (2004) NCST No 45.

36 KEMRI Standard Operating Procedure for Secondary Use of Samples (KEMRI/SERU/SOP/PI/SUBS) Version 1.0 Dated 18 October 2017.

Regulation of data protection in Kenya

Part XV of the Health Act 2017 is entirely devoted to E-Health and section 104 requires the enactment of a number of pieces of legislation within 3 years of the Act coming into force, including legislation on the protection of privacy and legislation on the collection and use of personal health information.

The Access to Information Act 2016 provides citizens with the right to access information held by the State or another person where the information is required for the exercise and protection of any other right or fundamental freedom. It defines personal information as information about an identifiable individual and genetic information would thus fall under this definition. Under section 5(1), a public body (of which KEMRI is) must make available the procedure to be followed when determining access to information and the chief executive officer of a public body is designated as the Information Access Officer (section 7.1). The Commission of Oversight and Enforcement has a number of functions under the Act and they pertain to both the right to access information and the right to the protection of personal information. Unlike in South Africa, the impact of the Access to Information Act 2016 on medical research is rather limited and likely only applies to having policies in place to facilitate access to information.

Data Protection Bill 2018

Kenya has introduced a Data Protection Bill, 2018. The purpose of the Bill is to give effect to the constitutional right to privacy, establish the Office of the Data Protection Commissioner, regulate the processing of personal data, provide for the rights of data subjects and obligations of data controllers and processors, and regulate the flow of personal data across borders. While seeking to protect the right to privacy, the Bill recognizes that the right is not absolute and specifically can be limited in order to safeguard the rights and freedoms of others and maintaining law and order. Section 6(2) also states that the right to privacy may be limited, including for purposes of public interest. The 'public interest' is undefined and it is unclear whether research would come under this exception.

There is a general prohibition on the processing of special information and this includes biometric data, but section 24(2) provides for a number of exemptions and this includes processing for research purposes. The processing of personal information relating to a data subject's health is limited by section 24. In the research context, it is only possible if the processing is for the purposes of treatment and care of the data subject.

A data subject is conferred with a number of rights including the right to be informed about the purpose of the processing of their personal data, access the data, object to the collection or processing of the data, correction of false or misleading data, deletion of false or misleading data that has been objected to, and 'an explanation in respect of the processing of data and the outcome of such processing' (section 9).

Prior to collection of personal data, the agency must inform the data subject that their data is being collected, the purpose and use of data collection, the intended recipients of the information, the name and address of the agency holding the data, whether any other agency will receive the data, and about the right to access (section 10). However, these rights and duties do not have to be followed if the data subject authorised the collection of the data from a third party (section 12(b)), if non-compliance does not prejudice the interests of the data subject (section 12(c)), compliance is not reasonably practicable in the circumstances of the case (section 12(f)), or the information is used for research purposes and will not be published in a form that could reasonably be expected to result in the identification of the data subject.

This is of particular important in determining the legal status of broad consent. Under section 4, one of the principles of the protection of personal data is that the 'information shall not be distributed in a manner that is incompatible with the purpose for which it was collected with the consent of the person'. Section 7(1) requires that data be collected directly from a data subject and that it must be for a lawful and specifically defined purpose. There are exemptions from the requirement that data be directly collected from the data subject and this includes where the data subject consents (section 7(2)(b)), collection from another source would not prejudice the interests of the data subject (section 7(2)(d)), or compliance with this section is not reasonably practicable in the circumstances of this case (section 7(2)(f)). If biorepositories seek to share based on section 7(2)(d) or 7(2)(f), they would need to demonstrate that they meet these requirements and this should be recorded. However, biorepositories are more likely to rely on the research exemption contained in section 12(f).

There is one possible challenge to the permissibility of broad consent and this is contained in section 20 which states that unless provided by the Bill or any other law, 'an agency that holds personal data that was obtained in connection with one purpose shall not use the data for any other purpose'. Arguably data that was

obtained for research and is to be used for research would satisfy the requirements of this section, particularly considered the wider regulatory environment for health research in Kenya that permits the use of broad consent. Clarity would undoubtedly be welcomed, but one could tentatively assume that, if this Bill is passed, broad consent continues to be legally permitted.

Under section 15, an agency (ie a person who collects or processes personal data) must take steps to protect the security of personal data. They must identify risks and establish safeguards. Section 19(1) states that an agency may not retain information for a period longer than that necessary to achieve the purpose of processing, but this can be waived if processing is for research (section 19(2)(c)). The commercial use of the data is prohibited unless the data subject has consented, or it is authorized to do so by law, and the data subject is aware of that (section 21). There is no research exemption for this provision, thus limiting the commercial use of the data.

Finally, the conditions for the transfer of data out of Kenya are strict and the following must be met: the third party is subject to laws or an agreement that puts in place adequate measures to protect personal data, the data subject consents to the transfer, the transfer is necessary for the performance of a contract between the agency and third party, and the transfer is for the benefit of the data subject.

KEMRI Centre for Geographic Medicine, Coast (CGMRC), one of 12 centres for KEMRI, have developed a policy on data protection that adopts principles based on the UK Data Protection Act, the EU General Data Protection Regulation and the Kenyan Data Protection Bill (2012).[37] The policy is aligned with the 2012 Bill, but will be updated once the 2018 Bill is passed. The policy outlines the obligations in terms of confidentiality and privacy and outlines the considerations to be made in case of a potential breach.

Sharing of data with KEMRI: some observations

The national and local regulations that apply to KEMRI provide clear guidance on the conduct and oversight of research, including obtaining biological samples. However, the considerations and requirements on biorepositories are not fully addressed and, until the Bill is passed, there is little consideration of the sharing of health data for research. For now, if the NSB wishes to continue to share health data with KEMRI, it must have a MTA in place that meets the requirements under South African law. This must detail the rights of the data subject and the procedures to be followed to ensure compliance with the provisions under POPIA.

The 2018 Kenyan Bill does provide for a clearer research exemption than the POPIA and in this respect is much more friendly for research. It is likely that once the Bill is enacted it will provide a sufficient level of protection to facilitate the cross-border flow of data between Kenya and SA, but clarity on the legal status of broad consent under the Bill would be necessary. The NSB should continue to require a MTA as the Kenyan Bill does not satisfy other SA regulatory requirements, notably the requirement of a MTA in the sharing of data.

The regulation and protection of data sharing for health research in Nigeria

The guarantee and protection of privacy is constitutionally protected in Nigeria pursuant to section 37 of the Constitution.[38] The obligation of privacy often has broad application, which could be interpreted to include information privacy.[39] However, the Constitution does not define privacy or specify how this constitutional right applies to information privacy.[40] Nigeria's Constitution also does not explicitly create a right to access personal information.

The National Health Act 2014 (NHA) enumerates rights and obligations of healthcare personnel.[41] Section 26 dictates that all health care users' information is confidential.[42] User information cannot be disclosed outside of the ordinary course and scope of business unless there is user consent, a court order or equivalent, or a threat to public health.[43] Persons with access to health records must protect them from unauthorized users and shall not duplicate information, links personal identifiers with other information, or gains access to health records or record-keeping systems without authority.[44] Users and staff may make formal complaints to this regard, through the Laying of Complaints

37 <http://constitutionnet.org/sites/default/files/the_data_protection_bill_2012_revised_10th_jan2012.pdf> accessed 31 May 2019.

38 S 37 'Constitution of the Federal Republic of Nigeria 1999' <http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm> accessed 31 May 2019.

39 Alex B Makulilo, *African Data Privacy Laws* (Law, Governance and Technology Series, vol 33, 2016).

40 Ibid.

41 National Health Act 2014 <http://lawnigeria.com/LawsoftheFederation/National-Health-Act,-2014.html> accessed 31 May 2019.

42 Ibid s 26.

43 Ibis ss 26 and 27.

44 Ibid s 29.

procedure, which is to be established and displayed and/or communicated in health establishments.[45] These provisions have limited applicability to biorepositories as many biorepositories do not provide health services.

The NHA authorizes the National Health Research Ethics Committee (NHREC) to establish guidelines for HRECs.[46] The NHREC's primary role is to protect human research participants' in Nigeria.[47] More specifically, NHREC establishes guidelines for conducting research, adjudicates complaints from and against local HRECs, and recommends courses of action where there are violations of standards, guidelines or relevant Acts.[48] NHREC Code is applicable to all human research 'conducted, supported, or otherwise subject to regulation by any institution in Nigeria'.[49]

Institutions or entities involved in human research must either establish an institutional HREC, register with a nearby local HREC, or register with the NHREC.[50] HREC or NHREC approval or exemption is required for the conduct of human research. Research involving the collection or use of data and/or specimens if the information is publicly available, or if the information does not exist in a manner that identifies participants directly or via identifiers associated with participants are exempt.[51] NHREC Code requires the submission and review of consent forms, and lays out requirements for consent forms and informed consent.[52] NHREC Code also requires submission of a MTA where biological materials are exported out of Nigeria, but there is no national MTA template.[53] The MTA must outline the terms of agreement and be signed by both parties, their affiliated institutions, and other related institutions. The MTA does not eliminate participants' rights to withdraw their specimen from research. Although the NHREC Code does not specify requirements for data protection, it does refer to and enforce relevant statutes. Thus, NHREC could play a major role in the implementation of future laws. The role of the NHREC is to review, approve, disapprove, request modification and monitor all relevant aspects of human subjects' research to protect participants.

In 2013 the NHREC developed a Policy Statement on Storage of Human Samples in Biobanks and Biorepositories in Nigeria.[54] Although much of the provisions discuss biological samples and not data, the policy does speak of anonymized and de-identified data. Importantly for biorepositories, the policy explicitly states that it supports broad consent (section E.1).[55]

Nigeria Data Protection Regulation 2019

The National Information Technology Development Agency (NITDA) was founded by the Government of Nigeria to implement information technology (IT) related policies and serves as the premier authority for standards, guidelines and policies related to IT.[56] In 2019, NITDA issued the Nigeria Data Protection Regulation 2019 to protect personal data privacy.[57] The Regulation defines personal data as including genetic information and physical and physiological features that may identify an individual, as well as, personal identifiable information, which can identify an individual if combined with other information.[58] It applies to natural persons in or residing in Nigeria and transcends borders where data of individuals of Nigerian descent is processed.[59] The Regulation establishes common principles such as lawful processing, purpose limitation, data accuracy, storage limitation, data security and accountability.[60] Processing of personal information is lawful where there is consent, necessity for performance of a contract, a legal obligation, or a need to protect the interest of the data subject, another natural person, or the public.[61] Consent is defined as any 'freely given, specific, informed and unambiguous indication of the data subject's wishes' and data must be collected for a 'specific, legitimate and lawful purpose'. Further processing is only permitted if further processing is for scientific research, public interest, or archiving.[62] This does not appear to permit broad consent as section 3.1(7)(m) states that if the Controller intends to process data for a purpose other than for what the data was collected, the data subject must be provided with that information in advance of the processing.

45 Ibid s 30.

46 Ibid s 33.

47 National Code of Health Research Ethics 2007 <http://www.nhrec.net/nhrec/NCHRE_Aug%2007.pdf> accessed 31 May 2019.

48 About Us 'National Code of Health Research Ethics' 2007 <http://www.nhrec.net/nhrec/NCHRE_Aug%2007.pdf> accessed 31 May 2019.

49 Ibid s A.

50 Ibid s C.

51 Ibid s B.

52 Ibid s E.

53 Ibid s E(n).

54 NHREC, *Policy Statement on Storage of Human Samples in Biobanks and Biorepositories in Nigeria* (PS1.02013).

55 For more on the regulation of biorepositories in Nigeria see O Nnamuchi, Biobank/Genomic Research in Nigeria: Examining Relevant Privacy and Confidentiality Frameworks (2015).

56 Background page National Information Technology Development Agency <https://nitda.gov.ng/nit/background/> accessed 31 May 2019.

57 S 1.1 'Nigeria Data Protection Regulation 2019' <https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf> accessed 31 May 2019.

58 Ibid s 1.3.

59 Ibid s 1.3.

60 Ibid s 2.1.

61 Ibid s 2.2.

62 Ibid s 2.1(1)(a)(i).

The Regulation resembles POPIA in the affirmative rights bestowed to data subjects and the responsibilities required of controllers, such as biorepositories. Data subjects have rights to access, erasure, restriction, objection, data portability, file a complaint, and seek redress.[63] Data Controllers define the purpose and methods to collect data,[64] conduct assessments to determine and mitigate risks,[65] conduct and report audits,[66] ensure continuous capacity building,[67] respond to donor requests and complaints, report breaches to the Agency, and hire a Data Protection Officer (DPO).[68] The DPO ensures compliance to the Regulation.[69]

Similar to POPIA, the Regulation imposes limitations on third party and international sharing. Under the Regulation, third party processing must be governed by a written contract between the Controller and the third party.[70] Additional requirements for international transfer of personal information are based on adequacy decision of the country or sector, Honorable Attorney General of the Federation (HAGF) decision of country/sector policies, implementation of such laws (including onward transfer to other country), existence and effectiveness of at least one authority in the country for ensuring compliance and cooperation, and legal obligation (ex. Convention).[71] There are exceptions where the data subject consents, or where personal information is required to perform a contract, for public interest, to support legal claim, or in the vital interest of the data subject.[72]

The Regulation bares many similarities to POPIA. The Regulation is based on principles of accountability, use for purpose, relevance, and etc. that are expressed in GDPR. The Regulation, like POPIA requires consent or contract to perform research with data and/or biospecimen containing personal information. Personal information includes genetic information. There is a research exception that would enable biorepositories to perform and share samples for additional testing. However, sharing with third parties must be subject to a contract. The Regulation does not specify a requirement for an MTA as POPIA; however; they both represent agreements between the Controller and the recipient. Similarly, international sharing is permissible via an adequacy decision by the agency, case by case review and approval of policies of the country/sector/authority in the relevant area, consent, or contract. Under the Regulation it is unclear if a general statement in the consent form of the intent of international sharing would suffice to enable international sharing. In any case the Controller is primarily responsible for establishing and the system for data processing, ensuring compliance of third party recipients, attending to requests and complaints, and reporting breaches.

Nigeria Protection of Personal Information Bill 2016

The Nigeria Protection of Personal Information Bill was introduced in 2016 but has not been passed. If the Bill is passed, it will provide a universal data protection law for Nigeria and will supersede the 2019 Regulation. Personal information is defined as information that relates to an identifiable living, natural person and an identifiable juristic person.[73] Biorepositories can process personal information by consent or contract.[74] Personal information includes biometric information, blood type, and other features of health. Whereas, the inclusion of genetic information can be reasonably inferred from the definition of *special personal information*, which includes 'information concerning inherited characteristics'.[75] Thus, like POPIA, biometric and genetic information are regulated. Similarly, the Bill prohibits the processing of special personal information, but enables biorepositories to process the information via in exception for scientific research.[76]

Chapter three of the Bill enumerates eight principles of information protection that are identical to those set out in POPIA: accountability, process limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, data subject participation.[77] However, a biorepository does not have to adhere to the retention limitation if the information is used for research purposes and it has adequate safeguards in place.[78] Biorepositories may also perform additional processing of personal information pursuant to the research exception if the information is

63 Ibid s 3.1.
64 Ibid s 1.3.
65 Ibid s 4.1(5).
66 Ibid ss 4.1(6–7).
67 Ibid s 4.1(3).
68 Ibid s 4.1(2).
69 Ibid.
70 Ibid s 2.7.
71 Ibid s 2.11.
72 Ibid s 2.12.
73 S 1 'Nigeria's Protection of Personal Information Bill 2016' <https://www.nassnig.org/document/download/8938> accessed 31 May 2019.
74 Ibid ss 10–15.
75 Ibid.
76 Ibid s 30.
77 Ibid Ch 3.
78 Ibid s 14.2.

only used for research and identifiable information is not published publicly.[79] International transfer requires that the recipient is subject to similar laws, including pertaining to further transfers.[80] The Bill also permits the Information Protection Regulator to allow for the processing of information despite the potential for a breach of a principle of data protection on a number of grounds, including research.[81]

The Bill resembles POPIA regarding the rights it grants data subjects and the responsibilities required of responsible parties, such as biorepositories. Data subjects have the right to access, restrict, rectify, delete and object to processing of personal information, as well as the right to complain.[82] Biorepositories are generally tasked to maintain confidentiality, ensure compliance and report to the national governing body the 'Regulator'.[83] As such, the biorepository must register with the Regulator and submit relevant information such as the purpose of research, types of information collected, intent to share, and others as appropriate.[84] The biorepository must also respond to complaints and requests of data subjects pertaining to personal information; [85] protect information from unauthorized use, loss, destruction and damage;[86] effect rectification or erasure a required;[87] report potential and/or suspected unauthorized access[88] and report breaches to the data subject and the Regulator.[89] Biorepositories must also ensure statutory compliance is maintained by external entities with whom they share data, whether locally or internationally,[90] and follow specific procedures as required under the Bill.[91]

The Bill and POPIA have similar scope with regards to biorepositories and research. The laws have international application where there is trans-border data flow. Both require consent or contract to conduct research on personal information but exclude regulatory compliance where data is de-identified. Covered information includes genetic information, biological samples, and biometric information. Both enable biorepositories to process special information such as genetic information via a research exception. Moreover, the rights afforded to donors and the responsibilities assigned to controllers are synonymous. Lawful processing allows for secondary use and international sharing via consent, however international sharing is only permissible if the recipient is subjected to adequate data protection laws.

Sharing of data with Nigeria: some observations

Similar to SA, the regulation of data for health research in Nigeria is fragmented with no sector specific guidance. Due to the introduction of the 2019 Regulation, it is unclear what the status of the Data Protection Bill is and whether it will be passed any time soon. Although welcomed as providing a statutory basis for data protection in Nigeria, it is only a regulation and as such can be superseded by another other Act that is passed. A second issue is that broad consent does not appear to be permitted under the Regulation.

As the law currently stands, the statutory framework is likely to satisfy the requirements for the international sharing of data under POPIA. However, the NSB may not be able to share data with Nigeria that was obtained under broad consent. It is unclear whether the NHREC Policy will override the strict requirements regarding consent in the Regulation and further clarity on this matter is necessary. Similar to sharing data with Kenya, the NSB must ensure that it has a signed MTA in place that meets the requirements of the national MTA.

Conclusions

The strengthening of data protection through the introduction of legislation or regulations in SA, Kenya and Nigeria is to be welcomed and in particular will give effect to the constitutional right to privacy in all three jurisdictions. The challenge facing these and other countries in Africa that are strengthening their data protection regulations is similar to the experiences elsewhere, is that the data protection instruments reviewed here are omnibus and general legal frameworks, and as such, do not necessarily consider the particular nuances that are important in the oversight of health data research. Provisions are made for research, particularly in POPIA and the Kenyan Data Protection Bill, but sectoral specific guidance on the use and oversight of the sharing of data for health research is required. The

79 Ibid s 15(3)(e).
80 Ibid s 69.
81 Ibid 34(2)(e).
82 Ibid s 3.1.
83 Ibid s 21.
84 Ibid ss 51.
85 Ibid s 17.
86 Ibid ss 18 and 14.
87 Ibid ss 23 and 55.
88 Ibid s 21.
89 Ibid
90 Ibid ss 19–20.
91 Ibid s 51.

sectoral specific guidance that does exist in SA, Kenya and Nigeria generally focus on biological samples with little or no consideration for data.

For now, the NSB must remember that when POPIA comes into force it will impact on its sharing of data for research, but POPIA does not exist in isolation and the NSB must continue to follow the additional regulatory instruments in the regulation and oversight of health research in SA. A review of all its practices, procedures and work flows from data protection impact assessments, a review of its consent forms, through to bringing its MTA in line with the national MTA template is necessary. It is likely that this review will be necessary for all biorepositories across SA.

Looking beyond SA, although this article only reviewed regulations in Kenya and Nigeria the data protection instruments emerging do appear to follow similar principles and afford the data subjects similar rights. In such situations, the requirements under POPIA are met. Where no appropriate regulation is in place or a Bill has not been enacted (such as currently in Kenya), the NSB must ensure that the MTA stipulates the rights, duties, and obligations of the overseas biorepository with whom they are sharing their data. It is thus advisable that the NSB and other biorepositories in SA have a template MTA available for biorepositories in jurisdictions that have similar data protection regulations in place and jurisdictions that current have no data protection regulations.

Finally, despite the data protection regulations in place in jurisdictions to which it is sharing data, the NSB must ensure that the MTA ensures that the recipient organization is bound by the duties and responsibilities beyond POPIA. Thus, while POPIA may change the regulation of data protection for health research generally, it is the MTA that is likely to be of more importance in the sharing of health data for research across SA's borders.

doi:10.1093/idpl/ipz024